REMARKS/ARGUMENTS

Applicants submit this substitute amendment in place of the June 19, 2006 amendment (which was not entered). Applicants are concurrently filing a Request for Continued Examination requesting entry of this substitute amendment.

Entry and consideration of the foregoing amendments is respectfully requested. Claims 10–153 are cancelled without prejudice to further prosecution in a continuation, continuation-in-part, divisional or other related application. Claims 1–3, 5–9 remain pending in the present application.

Independent claim 1 was amended to recite methods for establishing secure communication between a calling party, such as a client, and a called party, such as a server. The amended claims consist essentially of the unique limitations including: identifying a calling party to a called party; generating a public-private key pair by the called party; transmitting a message including said a first shared random number and a public portion of the public-private key pair, which message is encoded with a symmetric encryption key; transmitting a message including a second shared random number, which message is encoded with the public portion of the public-private key pair; and obtaining a shared secret key from an output of a combining function having a first input including the first shared random number and having a second input including the second shared random number. Support for these amendments can be found in the specification in paragraphs [0056] through [0062].

All claims remain rejected for reasons already of record, as the Examiner rejected the arguments made in the Applicant's Amendment and Response mailed 23 December 2005 in the Final Office Action mailed 17 March 2006. The present rejections are respectfully traversed in view of the following arguments.

The Applicant respectfully submits that the cited prior art does not show or suggest methods for establishing secure communication consisting essentially of, *inter alia,* generating a public-private key pair by the called party; transmitting a message including said a shared random number and a public portion of a public-private key pair, which message is encoded with a symmetric encryption key; transmitting a message including a second shared random number, which message is encoded with the public portion of the public-private key pair; and obtaining a shared secret key from an output of a combining function having a first input including the first shared random number and having a second input including the second shared random number.

In particular, the cited prior art nowhere shows or suggests using two shared random numbers in a series of communications including a communication that is encrypted using a symmetric encryption key that also includes a first shared random number and the public portion of a public-private key pair with transaction; and another communication in which the second shared random number is encrypted using the public portion of the key pair. The present invention is thus able to establish secure, validated communications with no more than three (3) transactions.

In contrast to the present invention, the cited prior art, especially Bellovin, teaches the use of an additional encryption key *R,* which is not used and has no equivalent in the present invention, in combination with the shared random numbers S_A and S_B. See Bellovin at Columns 5–6. The use of the additional key, *R*, requires five (5) transactions, three of which are encrypted using *R*, to achieve the results of the present invention.

Thus, the present invention provides a simpler and computationally faster method for establishing secure communication than shown or suggested by the prior art. Moreover, because the present invention can establish secure, validated communication in three (3) transactions as opposed to the five (5) taught by the cited prior art (Bellovin), the present invention is much less susceptible to a third party breaking the invention's encryption since the cryptically relevant information is exchanged fewer times compared with the methods of the cited prior art.

Conclusion

In view of the foregoing, it is respectfully submitted that the above-identified patent application is in condition for allowance. A Notice of Allowance is therefore respectfully requested. The Examiner is encouraged to contact the undersigned at the telephone number provided below to resolve any remaining questions or issues.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Robert W. Faris/
Robert W. Faris
Reg. No. 31,352

RWF:ejs
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100